

The invention claimed is:

1. A system for controlling access of an individual to an area, the individual having a unique biometric identifier, said system comprising:

a computer in communication with a database, said database having stored biometric identifier information contained therein;

a profile-generation application executable by said computer, said profile-generation application automatically generating a profile for the individual, said profile comprising at least one rule for controlling access to the area by the individual; and

a verification application for comparing said individual biometric identifier with said stored biometric identifier information in said database for determining whether to allow access to the area to the individual as in accordance with said at least one rule.

2. The system of claim 1 further including an enrollment application executable by said computer for transferring said individual biometric identifier to said database for enrolling the individual in the system.

3. The system of claim 1 wherein there are one or more additional applications executable by said computer and said profile-generation application changes said profile for the individual in response to the results of said one or more additional applications.

4. The system of claim 3 wherein said one or more additional applications comprise a data mining application that searches said database to correlate activity patterns of the individual for determining whether a rule violation has occurred.
5. The system of claim 1 further including an identification instrument issued to the individual, said identification instrument containing the biometric identifier of the individual, whereby the individual may present the identification instrument for verification.
6. The system of claim 5 wherein said computer is a central computer and said database is a central database, said system further including a peripheral station having a peripheral computer in communication with said central computer and said central database, said peripheral computer being in communication with a peripheral database, whereby a reader is in communication with said peripheral station for reading said individual biometric identifier stored in said identification instrument, and whereby, if said peripheral computer is unable to communicate with said central computer for verification, access to the area is denied to the individual.
7. The system of claim 1 wherein said computer is a central computer and said database is a central database, said system further including a peripheral station having a peripheral computer in communication with said central computer and said central database, said peripheral computer being in communication with a peripheral database, whereby an enrollment application is executable by said peripheral

computer for transferring said individual biometric identifier to said peripheral database for enrolling the individual in the system, and whereby said peripheral database is automatically synchronized with said central database for completion of enrolling of the individual.

8. A method for controlling access of an individual to an area, said method comprising:

enrolling the individual for access to the area by obtaining personal information, including personal biometric information, from the individual;

generating a profile comprising at least one rule for controlling the individual's access to the area;

storing activity data of the individual in a database;

performing data mining of said database to detect a pattern of activity by the individual, whereby said data mining produces a result; and

automatically generating a new profile comprising at least one rule for controlling the individual's access to the area based on said result of said data mining.

9. The method of claim 8 further including the step of providing the individual with an identification instrument, said identification instrument including said personal biometric information to aid the system in verifying the identity of the individual.

10. The method of claim 9 wherein said step of storing activity data includes storing a record of transactions performed by the individual when using said identification instrument to access the area.

11. The method of claim 9 wherein said personal biometric information comprises fingerprint data, and said identification instrument is a smart card containing encoded fingerprint data of said individual.

12. A method for controlling access of an individual having a personal biometric identifier to an area, said method comprising:

- providing the individual with an identification instrument, said identification instrument containing said personal biometric identifier;

- providing a database containing stored biometric identifier information, said stored biometric information including said personal biometric identifier of said individual;

- automatically generating a profile comprising at least one rule for controlling access of the individual to the area;

- applying said at least one rule when comparing said biometric identifier contained in said identification instrument with said biometric information in said database to verify the authenticity of said identification instrument for determining whether to grant access to the area to the individual.

13. The method of claim 12 further including the step of providing said identification instrument with a microprocessor, wherein said personal biometric identifier comprises fingerprint data, and said identification instrument is a smart card containing encoded fingerprint data of said individual.

14. The method of claim 12 further including the step of 6 virtually compartmentalizing said database so that an operator can perform data mining operations on said database without compromising an identity of an individual whose pattern of activity is under investigation.

15. A hierarchical system for controlling ingress and egress to an area by an individual having a biometric identifier, said system comprising:

a reference database containing stored biometric identifier information;

a computer in communication with said database;

a biometric identifier information input;

an enrollment application executable by said computer for storing enrollment information in said reference database, said enrollment information including said biometric identifier information of the individual; and

a profile generator application executable by said computer for automatically generating a hierarchical profile in response to said enrollment information, whereby said generated hierarchical profile comprises at least one rule for controlling the individual's ingress and egress to the area, whereby the system will automatically control the ingress and egress of the individual to the area on the basis of said

hierarchical profile when the individual's said biometric information is presented to said biometric information input unit.

16. The system of claim 15 further including a data mining application executable by said computer, said data mining application monitoring an access activity of the individual to the area for determining if said access activity constitutes a rule violation.

17. The system of claim 16 wherein if said access activity constitutes a rule violation, said data mining application issues an alert and said profile generator application generates a new hierarchical profile for the individual.

18. The system of claim 15 wherein said system includes a central system and a peripheral system, and wherein said reference database is a central database and said computer is a central computer, and said peripheral system includes a peripheral database and a peripheral computer, whereby said peripheral computer is enabled to receive said enrollment information and transfer said enrollment information to said peripheral database for generating an initial hierarchical profile comprising at least one rule controlling the individual's ingress and egress to the area, and whereby said enrollment information is transferred to said central computer for generating a new hierarchical profile comprising at least one rule regarding the individual's ingress and egress to the area.

19. The system of claim 15 further including an identification instrument containing said biometric identifier information of the individual, said identification instrument being capable of communicating said biometric identifier information to the system in a contactless manner.

20. The system of claim 15 wherein said database is virtually compartmentalized so that an operator can perform data mining operations without compromising the identity of an individual whose pattern of activity is being investigated